Verification of Key Generation from Individual OFDM Subcarrier's Channel Response

Verification of Key Generation from Individual OFDM Subcarrier's Channel Response

Junqing Zhang*, Roger Woods*, Alan Marshall§, Trung Q. Duong*
* ECIT, Queen's University Belfast
Belfast, BT3 9DT, UK
Email: {jzhang20, r.woods, trung.q.duong}@qub.ac.uk
§ Department of Electrical Engineering and Electronics, University of Liverpool
Liverpool, L69 3GJ, UK
Email: Alan.Marshall@liverpool.ac.uk

***Abstract*—This paper presents a key generation system derived from the channel response of individual subcarrier in orthogonal frequency-division multiplexing (OFDM) systems. Practical aspects of the security were investigated by implementing our key generation scheme on a wireless open-access research platform (WARP), which enables us to obtain channel estimation of individual OFDM subcarriers, a feature not currently available in most commercial wireless interface cards. Channel response of individual OFDM subcarrier is usually a wide sense stationary random process, which allows us to find the optimal probing period and maximize the key generation rate. The implementation requires cross layer design as it involves interaction between physical and MAC layer. We have experimentally verified the feasibility and principles of key generation, and also evaluated the performance of our system in terms of randomness, key generation rate and key disagreement rate, which proves that OFDM subcarrier's channel responses are valid for key generation.**

I. Introduction

Wireless communication is vulnerable due to its broadcast nature. Physical layer security (PLS) which aims to achieve perfect secrecy therefore has been received extensive research interest [1]. PLS research mainly can be divided into two branches: secret key-based secrecy [2], [3] and keyless security based on Wyner's wiretap channel [4]. However, keyless security schemes usually require full/part channel state information (CSI) of eavesdroppers, which is not always available in practice [5]. Therefore, there has not been any practical implementation of keyless security schemes reported.

Secure key generation from noisy channels, an active research direction of secret key-based secrecy, is one of the few PLS techniques that have been reported to be implementable in current commercial wireless devices [6], [7]. This technique exploits the randomness of common wireless channels to establish secure keys at each side of a link between two legitimate users. It does not require perfect CSI, as the users are able to reach an agreement on keys through public discussion [8]. Encryption key is traditionally shared by public key cryptography, which is computationally secure. In contrast, key generation is information-theoretic secure [3], which is a promising technique to establish encryption keys.

There have been several practical key generation systems reported, employing IEEE 802.11 [9]–[14], IEEE 802.15.4 [15]–[18], ultrawideband (UWB) [19], TV and radio signals [20]. IEEE 802.11 is the most widely adopted wireless technique in key generation due to its widespread application in our daily life. Received signal strength (RSS) is currently the most popular parameter used for key generation [9]–[11] because it is available in off-the-shelf commercial WiFi network interface cards (NICs). However, RSS-based systems suffer from a low key generation rate (KGR) as this approach only extracts randomness from a single dimension. CSI-based systems can provide a higher KGR as CSI is a finer-grained channel parameter [21]. However, CSI is not available in most WiFi NICs with the current exception of Intel WiFi Link 5300 wireless NIC [22], which makes key generation from CSI feasible [12], [13]. As the Intel WiFi Link 5300 wireless NIC supports IEEE 802.11n, multiple-antenna diversity was used to exploit a finer-grained spatial channel characteristics [14]. There is also research interest using customized hardware platforms to extract randomness from some special parameters, for example, generating keys from the peak of the channel impulse response (CIR) by using an FPGA-based 802.11 platform [10].

Wireless sensor networks (WSNs) are another hot application area of key generation [15]–[18]. The CC2420 is a 2.4 GHz IEEE 802.15.4 compliant RF transceiver and widely used in WSN nodes, such as MicaZ and TelosB. CSI is not available in the IEEE 802.15.4 standard so only RSS-based key generation systems can be implemented. Also, because sensor nodes are usually constrained by computational capacity, energy consumption and low mobility, particular challenges arise in the application of key generation to WSNs, as special attention has to be paid to the design of the key generation scheme [15], [16]. There are also research efforts to extract keys in other wireless systems. The application of key generation in a UWB system was verified using a measurement system composed of an oscilloscope, a waveform generator, etc [19]. FM and TV signals were also used for key generation by employing universal software radio peripheral (USRP) for channel measurements [20].

Our work differs from [12], [13], which also extract keys from CSI. The work in [12] generates key from all the subcarriers. However this approach can introduce redundancy whenever the channel experiences flat fading, as this can

produce periodic runs of ones and zeros, leading to reduced randomness and hence security. The authors in [13] randomly select some key bits from the key streams generated from all the subcarriers and validate if the selected keys are the same at both users, which quickly becomes very inefficient whenever there are poor channel conditions, as a single key bit mismatch will result in a restart of the entire recombination process. We have proposed to generate keys from the channel responses of individual subcarriers in orthogonal frequency-division multiplexing (OFDM) systems, using a statistical channel model [23]. We have proved that channel response of individual OFDM subcarrier is usually a wide sense stationary (WSS) random process, which allows us to find the optimal probing period and maximize the KGR.

In this paper, we verify its feasibility through implementation on the wireless open-access research platform (WARP) [24] running an IEEE 802.11 OFDM PHY and a distributed coordination function (DCF) MAC. A key objective here is to make minimal or even no changes to the off-the-shelf wireless standard. This presents new research challenges, as it requires cross layer design. Our contributions are as follows:

- We propose a practical OFDM subcarrier's channel response-based key generation scheme implemented on the WARP hardware using data and ACKnowledgement (ACK) packets to measure the channel. This enables us to carry out the channel measurements without changing the IEEE 802.11 protocol, and ensures that the time difference between these measurements is kept very small. In this way, we can reduce the impact on channel reciprocity caused by asynchronous measurements.
- We have experimentally verified the key generation principles: temporal variation and channel reciprocity. We also evaluated the performance of our key generation system in terms of randomness, KGR, and key disagreement rate (KDR). Through the verification and performance evaluation, we find that OFDM subcarrier's channel responses are valid for key generation.

The rest of the paper is organized as follows. Section II introduces the related IEEE 802.11 PHY and MAC protocol, and the WARP hardware which we used in our implementation. Section III presents the test scenarios and WARP setup. We verify the key generation principles in Section IV and evaluate the performance of our key generation system in Section V. Section VI concludes the paper.

II. Preliminary

We implemented our OFDM subcarrier's channel response-based key generation system using WARP boards running the IEEE 802.11 OFDM and DCF MAC. In this section, we introduce the related IEEE 802.11 physical and MAC layer protocols and the WARP hardware platform.

A. Related IEEE 802.11 Protocol

1) OFDM PHY: The IEEE 802.11 a/g/n standards [25] adopt OFDM to modulate the signal. The physical layer packet of IEEE 802.11 OFDM consists of a preamble, a SIGNAL field, and a DATA field, as shown in Fig. 1. The preamble is used for automatic gain control (AGC), synchronization and channel estimation, and is equivalent to 4 OFDM symbols in length. The SIGNAL field carries the information of convolutional coding rate R and the mapping scheme for the DATA field and forms a complete OFDM symbol. The number of OFDM symbols of the entire physical layer packet can be calculated as

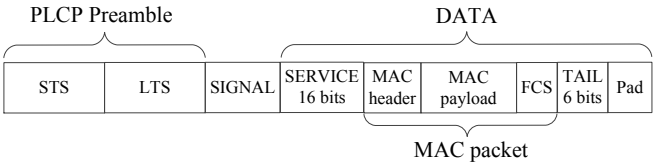

Fig. 1. Structure of IEEE 802.11 OFDM physical layer packet. The length of the blocks in the figure is not scaled.

$$N_{\text{OFDM}} = 4 + 1 + \lceil \frac{l_{\text{MAC}} \times 8 + 16 + 6}{N_{subc} \times N_{bpsc} \times R} \rceil, \tag{1}$$

where l_{MAC} is the number of bytes of the MAC packet, N_{subc} is the number of data subcarriers and equals 48 in IEEE 802.11 standard, and N_{bpsc} is the number of bits per subcarrier which is determined by the mapping scheme.

Least square channel estimation is widely used to estimate the channel with the aid of long training symbols (LTSs) in IEEE 802.11 OFDM system. The estimated channel can be given as

$$\widehat{H}_{uv}(f_m, t) = H_{uv}(f_m, t) + \widehat{w}_{uv}(f_m, t), \tag{2}$$

where f_m is the m^{th} subcarrier's carrier frequency, $H_{uv}(f_m, t)$ is the theoretical channel response, and $\widehat{w}_{uv}(f_m, t)$ is the noise effect for each subcarrier, u is the transmitter (Tx) and v is the receiver (Rx). The channel response of each subcarrier, i.e., $\widehat{H}_{uv}(f_m, t)$, provides information on the attenuation of each subcarrier/frequency by the channel and noise against time, which is an ideal randomness source for key generation.

2) DCF MAC: In IEEE 802.11, the DCF is used to coordinate access to the wireless medium, which is the basis of the standard carrier sense multiple access/collision avoidance (CSMA/CA) access mechanism. In order to ensure reliable reception of the unicast frame, a positive ACK frame is transmitted from Rx to Tx after waiting a short interframe space (SIFS) when Rx successfully receives a data packet from Tx, as illustrated in Fig. 2.

When IEEE 802.11 network is configured as an infrastructure basic service set (BSS), the network is handled by an access point (AP) that broadcasts Beacon frames to all the users, i.e., mobile stations (STAs), in its communication range, typically every 100 ms. The Beacon carries information about the BSS parameters, e.g., timestamp, service set identity (SSID), Beacon interval, etc. STAs can use these information to identify the network and keep synchronized to the AP.

B. WARP Hardware Platform

CSI is not made public in most commercial NICs. There is a Linux driver developed for the Intel WiFi Link 5300 wireless

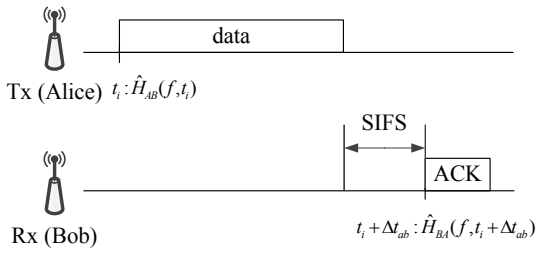

Fig. 2. Timing between data and ACK packet

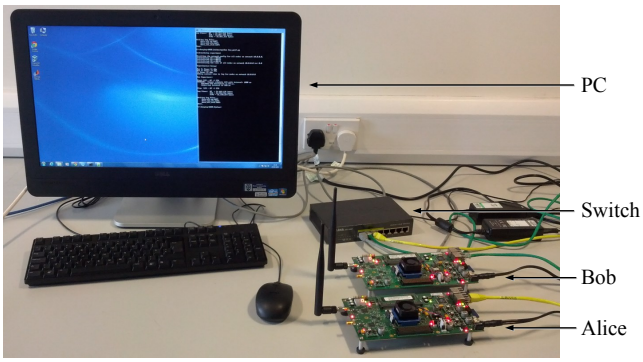

Fig. 3. The experiment system of the static scenario with two users (Alice and Bob).

NIC to access CSI [22], however, it still does not give users full access to all the transmission parameters.

We have adopted a customized hardware platform, WARP, which is a scalable and extensible programmable wireless platform and allows fast prototype of physical layer algorithms. The WARP team has developed an 802.11 reference design, which is a real-time FPGA implementation of the IEEE 802.11 OFDM PHY and DCF MAC for WARP v3 hardware. In order to control the behavior of the PHY and MAC without interfering with the real-time operation of the wireless interfaces, the WARP team has developed a Python experiments framework, which can log the transmission parameters, such as timestamp, rate, transmission power, received signal power, channel estimation, etc. In the experiments framework, WARP nodes are connected to a PC by a switch so the logged data can be saved in the PC for further processing. This enables us to verify the OFDM subcarrier's channel response-based key generation scheme on the WARP 802.11 reference design.

III. Design of the Measurement System

A. Test Scenarios

Alice and Bob are legitimate users attempting to establish keys between each other. The experiments were carried out in a lab with rich multipath, which is a typical indoor environment with cupboards, chairs, desks, etc. Alice was set to move randomly at a speed of about 1 m/s while Bob remained stationary. We also tested a static scenario with both users stationary. The experimental setup for the static scenario is shown in Fig. 3. The two WARP boards were connected to the PC by a switch so the data can be stored for off-line processing.

B. WARP Setup

Both Alice and Bob were running the WARP 802.11 reference design. They were operating at channel 1 of the 2.4 GHz carrier frequency. Alice and Bob were configured as AP and STA, respectively. As shown in Fig. 2, Alice sent data packets to Bob every 960 μs[1], which allows Bob to get a noisy estimation of the channel $\widehat{H}_{AB}(f, t_i)$. Bob was associated to Alice so he transmitted ACK packets to Alice on successful reception of unicast packets. The ACK is also modulated by OFDM so Alice can get the channel estimation $\widehat{H}_{BA}(f, t_i + \Delta t_{ab})$, where Δt_{ab} is the difference between the transmission time of the data packet sent by Alice and the corresponding ACK packet sent by Bob and can be calculated by

$$\begin{aligned} \Delta t_{ab} &= t_{\text{data}} + t_{\text{SIFS}} \\ &= N_{\text{OFDM}} \times \frac{80}{B} + t_{\text{SIFS}}, \end{aligned} \tag{3}$$

where B is the channel spacing, and t_{SIFS} is the time of the SIFS and equals to 16 μs in a 20 MHz channel spacing IEEE 802.11 OFDM system. In order to ensure a high correlation between the measurements of Alice and Bob, Δt_{ab} should be kept as small as possible. In the MAC packet, the MAC header is 24 bytes, frame check sequence (FCS) is 4 bytes, and the minimum MAC payload required by the WARP is 20 bytes, therefore we configured the length of the MAC packets l_{MAC} to be 48 in order to keep the duration of the packet as small as possible. Commercial WiFi systems will adjust data rate adaptively according to the channel condition, however, we configure the WARP system to run at the same rate in order to simplify the design. Ideally, the system should run at the maximum allowed rate, i.e., 54 Mbps, in order to minimize Δt_{ab}. However, it will suffer from a high bit error rate (BER) when the channel is bad so less packets will be correctly received. As a compromise, we ran the system at a rate of 18 Mbps, i.e., $R = 3/4$ and $N_{bpsc} = 2$. Δt_{ab} equals 60 μs when the system is configured as above. This time difference is very small and can ensure the environments experienced by the data packets and the corresponding ACK packets are almost the same. In a slow fading environment, this only contributes a very small displacement. When Alice is moving at a speed of 1 m/s, the distance she moves in this time interval is only 0.006 cm.

Alice broadcast Beacon frames every 100 ms which helped keep all of the users in the network synchronized. Bob can regularly update his timing through the timestamp received in the Beacon frames. This is quite important as there are frequency differences between the oscillators of different boards which results in a time drift and the timestamps of different users will deviate if they are not synchronized. There is no Tx address in the ACK packet, which can only be distinguished

[1]The WARP 802.11 reference design requires a transmission resolution of 64 μs.

by its temporal location compared to the timestamp of the data packets. Therefore, keeping users synchronized is essential to pair their channel measurements.

IV. Verification of Key Generation Principles

Key generation is based on three principles, i.e., temporal variation, channel reciprocity, and spatial decorrelation [9]. Temporal variation guarantees the randomness of the key sequence; channel reciprocity ensures that Alice and Bob can generate the same key sequence, while spatial decorrelation promises that an passive eavesdropper cannot get the same key sequence as either Alice or Bob. In this paper, we verified the first two principles by the data collected from the WARP boards. We ran all of the experiments for 300 s and sampled around 300,000 channel measurements for each user. The total experiment time is much larger than the coherence time of the channel, which is long enough to represent the channel variation and can get a high accurate correlation calculation. The amplitudes of the channel responses are used for the numerical calculation.

A. Temporal Variation

There are research efforts exploiting randomness from temporal, frequency and spatial domain. However, temporal variation is the most common and convenient source for key generation as the randomness can be simply introduced by the movement of the users and/or objects. Temporal variation can be quantified by the temporal autocorrelation function (ACF), which is defined as

$$R_{\widehat{H}_{uv}}(f_m, \Delta t) = \frac{E[|\widehat{H}_{uv}(f_m, t)||\widehat{H}_{uv}(f_m, t+\Delta t)|]}{E[|\widehat{H}_{uv}(f_m, t)|^2]}. \quad (4)$$

The temporal ACF describes how fast the signal decorrelates in the time domain. An interval that is too short between two adjacent measurements will result in redundancy and impact the randomness of the key sequence. An interval that is too long will result in a low KGR.

In a rich scattering multipath environment, the channel can be modelled as a *wide sense stationary uncorrelated scattering* (WSSUS) random process [26]. Under this assumption, we have already shown in [23] that OFDM subcarrier's channel response is a WSS random process. As a random process satisfies WSS property, data sampled by the same period will have the same correlation relationship.

$R_{\widehat{H}_{AB}}(f_1, \Delta t)$ and $R_{\widehat{H}_{BA}}(f_1, \Delta t)$ of the mobile scenario are selected as examples and shown in Fig. 4. As may be observed from the figure, the ACFs observed at t_1 and t_2 match each other, indicating that both $\widehat{H}_{AB}(f_m, t)$ and $\widehat{H}_{BA}(f_m, t)$ are WSS random processes, which is consistent with the simulation results in [23].

B. Channel Reciprocity

For a communication link between Alice and Bob, the signals observed at each end of the link are reciprocal. However, users need to detect and measure the received signal using hardware devices, most of which work in half duplex mode and introduce noise. Cross-correlation between their measurements can be used to describe the signal similarity, which is defined as

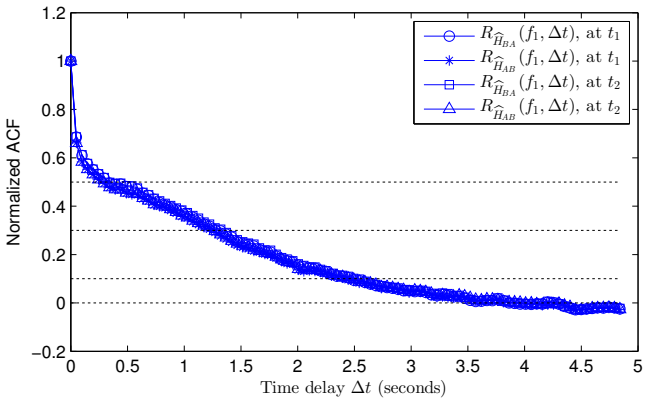

Fig. 4. Normalized temporal ACF of $\widehat{H}_{AB}(f_1, t)$ and $\widehat{H}_{BA}(f_1, t)$. $t_2 = t_1 + 10$ s.

$$\rho_{XY} = \frac{E\{XY\} - E\{X\}E\{Y\}}{\sqrt{E\{X^2\} - E\{X\}^2}\sqrt{E\{Y^2\} - E\{Y\}^2}}, \quad (5)$$

where $X = |\widehat{H}_{AB}(f_m, t)|$ and $Y = |\widehat{H}_{BA}(f_m, t + \Delta t_{ab})|$.

Cross-correlation is usually impacted by asynchronous measurements, noise, hardware difference, etc. Although most of the current commercial wireless devices cannot transmit simultaneously, the time difference of the measurements of Alice and Bob can be kept very small as described in Section III-B. Therefore, in a slow fading channel, the impact of asynchronous measurements can be minimized. The noise experienced in each user is independent and uncorrelated as it resides in two separate hardware devices. Therefore, noise represents the main factor that impacts the cross-correlation of the measurements.

The cross-correlation coefficients of static and mobile scenarios are shown in Fig. 5. In the static scenario, noises are the only contributor to the signal variation, therefore, the correlation coefficients of all the subcarriers are almost zero because noises are independent and uncorrelated. In the mobile case, the correlation relationship is much better as when Alice was moving the channel changed significantly. The correlation relationship is inversely proportional to KDR, which will be analyzed in Section V-D.

V. Performance Evaluation

A. System Overview

We use the same key generation system proposed in [23]. Both users exploit randomness from OFDM subcarrier's channel responses. A cumulative distribution function (CDF)-based quantization scheme is adopted to map the OFDM subcarrier's channel response to binary values. Secure sketch and universal hash function are used as information reconciliation and privacy amplification techniques, respectively.

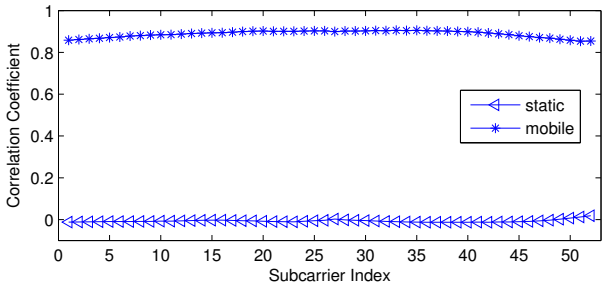

Fig. 5. Cross correlation in static and mobile scenario.

TABLE I
RANDOMNESS TEST RESULTS OF KEY SEQUENCES QUANTIZED FROM $\widehat{H}_{AB}(f_m, t)$. THE GREY CELLS FAIL THE RANDOMNESS TEST.

Corr coeff $X\%$	61.2%	48.3%	37.8%	32.4%	25%
T_p (s)	0.1	0.5	1	1.2	1.5
Sequence length	2978	598	298	248	198
Frequency	1	1	0.908	0.899	0.887
Block frequency	0	0.108	0.32	0.377	0.724
Runs	0	0	0.003	0.002	0.011
Longest run of 1s	0	0	0.184	0.137	0.258
DFT	0.112	0.058	0.41	0.641	0.493
Serial	0	0	0.051	0.098	0.185
	0	0.138	0.116	0.683	0.457
Appro. entropy	0	0	0.039	0.004	0.025
Cum. sums (fwd)	0.191	0.537	0.752	0.848	0.7
Cum. sums (rev)	0.191	0.537	0.643	0.733	0.831

B. Randomness

The generated key sequence is generally used for cryptographic applications. A key with redundancy results in a decrease of the security level of the data encryption. Therefore, randomness is the most important feature of the generated key sequence. We use National Institute of Standards and Technology (NIST) randomness test suite [27] to verify the randomness of the key sequence, which is also used by many other researchers [9], [10], [12], [13], [18].

There are 15 tests in total, each evaluating a specific randomness feature, e.g., frequency test focuses on the proportion of ones and zeros, DFT test detects the periodic feature of the sequence, etc. All the tests return a *P*-value, which is compared to a significance value α, whose typical value is in the range of [0.001, 0.01]. When *P*-value $> \alpha$, the sequence is accepted as random. We chose α as 0.01, the same as other work. Some of the tests require extremely long sequence, e.g., random excursions variant test recommends the input sequence longer than 10^6, which is currently not available in our experiments. Therefore, we ran 8 tests, which still satisfies the requirements of NIST.

The channel was originally sampled at a rate of 960 μs, at which rate there would definitely be redundancy between adjacent data samples. Therefore, we resampled the measurements by a period of T_p, quantized the resampled OFDM subcarrier's channel responses and finally applied the NIST randomness tests to the binary values.

The randomness test results are shown in Table I, where the grey cells fail the randomness test, i.e., *P*-value $< \alpha$. As may be observed from the table, when the correlation between the adjacent two measurements is high, the key sequence fails several tests. In this example, the system cannot generate a random key sequence until the probing period T_p reaches 1.5 s and the correlation coefficient between adjacent samples is 25%. The optimal probing period can be determined in this way rather than picking a large enough value, which could exploit the randomness as efficiently as possible.

C. KGR

As the generated key sequence is used for cryptographic application which requires a certain length of key sequence, the KGR will affect the practical application of key generation system. It is mainly determined by the variation of the channel, therefore, it does not make sense to compare KGR of two systems applied in two environments with different Doppler spread. KGR can be improved by extracting keys from a finer-grained channel information, e.g., OFDM subcarrier's channel responses. In this paper, we have verified the feasibility to extract keys from individual subcarrier. This approach has a major advantage over existing key extraction schemes, particularly in frequency-selective fading channels, whereby multiple subcarriers falling outside the coherence bandwidth can be explored in order to improve the KGR. Therefore, OFDM subcarrier's channel response-based key generation system can offer a better performance in terms of KGR compared to single dimension-based key generation systems, such as RSS-based systems.

D. KDR

KDR is the raw disagreement rate after quantization, which is defined as

$$KDR = \frac{\sum_{i=1}^{N} |K_A(i) - K_B(i)|}{N}, \tag{6}$$

where K_A and K_B are the quantized bits of Alice and Bob, respectively, and N is the length of keys. Information reconciliation is used to correct the mismatch, which is upper bounded by the correction capacity. For example, BCH code can correct up to 0.25 disagreement [28]. The KDR in static and mobile scenarios are shown in Fig. 6. As may be observed from the figure, KDR of all the subcarriers between Alice and Bob in the mobile scenario are within the BCH code's correction capacity (0.25). Therefore, Alice and Bob can agree on the same key after the information reconciliation stage. However, when all the users remained static, the KDR is around 0.5, which is no better than random guess. Therefore, in a static environment where noise is the only contributor to the randomness, it is not amenable to key generation.

VI. CONCLUSION

This paper presents a practical key generation system by exploiting randomness from OFDM subcarrier's channel responses. To the best of the authors' knowledge, this is the first paper that practically extracts keys from OFDM subcarrier's channel responses. In particular, we carried out the

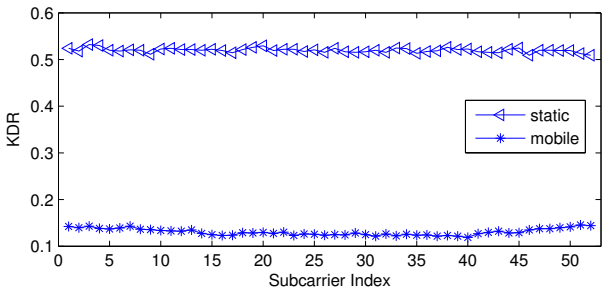

Fig. 6. Key disagreement rate in static and mobile scenario.

experiments by using WARP 802.11 reference design, which supports IEEE 802.11 OFDM PHY and DCF MAC. This enables us to extract OFDM subcarrier's channel responses through channel estimation. We configured the network as infrastructure BSS and used Beacon frames sent by the AP to keep all the users synchronized. The data and ACK packets were used to measure the channel and the time interval between the transmissions of these packets can be kept very small. In this way, we can suppress the effect on the channel reciprocity impacted by asynchronous measurements as small as possible. We have verified temporal variation and channel reciprocity. We have also evaluated the performance of our OFDM subcarrier's channel response-based key generation system in terms of randomness, KGR and KDR. Through the verification and performance evaluation, we find that OFDM subcarrier's channel responses are suitable for key generation. Verification of spatial decorrelation and key generation from multiple subcarriers will be our next step.

ACKNOWLEDGEMENT

The authors gratefully acknowledge support from the Queen's University Belfast scholarship, Newton Institutional Links Grant 172719890, Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, and US-Ireland R&D Partnership USI033 'WiPhyLoc8' grant involving Rice University (USA), University College Dublin (Ireland) and Queen's University Belfast (Northern Ireland). We also want to thank the WARP team for their continuous support, and Dr. Yuan Ding for his help on the experiments.

REFERENCES

[1] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography – Part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[4] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[6] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, 2015.

[7] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, pp. 1–12, Jan. 2015.

[8] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology-EUROCRYPT*, 1994, pp. 410–423.

[9] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. on Mobile Computing and Networking (MobiCom)*, Beijing, China, Sep. 2009, pp. 321–332.

[10] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th Annu. Int. Conf. on Mobile Computing and Networking (MobiCom)*, San Francisco, CA, USA, Sep. 2008, pp. 128–139.

[11] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842–1852, 2013.

[12] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. 32nd IEEE Int. Conf. on Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 3048–3056.

[13] W. Xi, X. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "KEEP: Fast secret key extraction protocol for D2D communication," in *Proc. 22nd IEEE Int. Symp. of Quality of Service (IWQoS)*, Hong Kong, May 2014, pp. 350–359.

[14] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. 29th IEEE Int. Conf. on Comput. Commun. (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[15] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1779–1790, 2013.

[16] S. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec. 2014.

[17] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, 2010.

[18] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, 2014.

[19] M. G. Madiseh, S. He, M. L. McGuire, S. W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *IEEE Int. Conf. on Commun.*, Dresden, Germany, Jun. 2009, pp. 1–5.

[20] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," in *Proc. 9th Int. Conf. on Mobile Systems, Applications, and Services (MobiSys)*, Washington, DC, USA, Jul. 2011, pp. 211–224.

[21] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, 2012.

[22] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: gathering 802.11n traces with channel state information," *ACM SIGCOMM Comput. Commun. Review*, vol. 41, no. 1, pp. 53–53, 2011.

[23] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Secure key generation from OFDM subcarriers' channel responses," in *Proc. IEEE GLOBECOM Workshop on Trusted Commun. with Physical Layer Security (TCPLS)*, Austin, USA, Dec. 2014, pp. 1302 – 1307.

[24] WARP Project. [Online]. Available: http://warpproject.org

[25] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 2012.

[26] P. Bello, "Characterization of randomly time-variant linear channels," *IEEE Trans. on Commun. Systems*, vol. 11, no. 4, pp. 360–393, 1963.

[27] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, Tech. Rep. Special Publication 800-22 Revision 1a, Apr. 2010.

[28] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "An effective key generation system using improved channel reciprocity," in *Proc. 40th IEEE Int. Conf. on Acoust., Speech and Signal Processing (ICASSP)*, Brisbane, Australia, Apr. 2015, pp. 1727–1731.